



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,299	12/05/2003	Wenbo Mao	B-5321 621552-2	2169

7590 10/19/2006

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER

LE, CANH

ART UNIT PAPER NUMBER

2112

DATE MAILED: 10/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

10/729,299

Applicant(s)

MAO ET AL.

Examiner

Canh Le

Art Unit

2112

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 22 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 21, 22, 24 and 25 is/are allowed.
- 6) ☒ Claim(s) 1-20, 23 and 26 is/are rejected.
- 7) ☒ Claim(s) 24 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 Dec 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 05 Dec 2003 3-29-04
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION*****Claim Objections***

Claim 24 is objected to because of the following informalities: "steps a) to c) being repeated as necessary to obtain  $s||w \leq N_A$ " appears twice in 24 c). "steps a())" should be replaced by "step a)" in 24 d). Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-15, and 16-19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claim 1 includes a function  $C1(\text{at least } m \text{ and } r)$  where  $C1()$  is a *deterministic combination function*. The deterministic combination function of variable at least  $m$  and  $r$  can be for example as the following:

$C1(m*m + n)$ ,  $C1(r*m - r*r)$ ,  $C1(m+r)$ ,  $C1(m-r)$ ,  $C1(m*r)$ ,  $C1(r||m)$ .

Art Unit: 2112

The subtraction and addition of two variables m and r are totally different than concatenation of m and r. Also the same reasons apply for *reversible combination functions* of C2(at least m and r) and function C3(at least m and r). There are many ways to combine m and r. Therefore, one of ordinary skill would not be able to make or use the invention without undue experimentation.

For claims 2-15, they are dependent on claim 1.

For claim 16, it relates to C1() deterministic combination function.

For claims 17-19, they are dependent on claim 16.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 9, 10, 13, 15, and 19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

For claim 9, the Examiner gives a broad interpretation of "the output of the combination function". It can be output of the deterministic function or the reversible function. Claim 9 recites the limitation "combination function" in line 4. There is insufficient antecedent basis for this limitation in the claim.

For claims 13 and 15, the inventor does not disclose a memory and processor that are used in these claims. Therefore, the Examiner has a question in his mind as to elements that are capable of carrying out the methods.

Art Unit: 2112

For claims 10 and 19, they have no elements. These claims are incomplete under 35 U.S.C. 112, second paragraph.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Regarding patent-eligible subject matter under 35 USC 101, claim 1 is directed to a practical application of a mathematical algorithm and not to mere manipulation of the algorithm itself. This is evidenced by the final result achieved being a digitally signed version of the message data string (via step d)) and under certain conditions an encrypted and digitally signed version (via step e)).

Claims 13 and 15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. They appear directed to an abstract idea rather than a practical application of the idea.

### ***Double Patenting***

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir.

Art Unit: 2112

1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 10, 11, 13, 15, 19, 20, 23, and 26 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 11, 12, and 14 of copending Application No. 10/468,687. Although the conflicting claims are not identical, they are not patentably distinct from each other because for the following reasons.

For claim 10, the Examiner gives a broad interpretation of apparatus for carrying out the method of claim 1. Claim 11 of Mao includes all items for this apparatus (the first computing entity).

For claim 19, the Examiner gives a broad interpretation of apparatus for carrying out the method of claim 16. Claim 12 of Mao includes all items for this apparatus (the second computing entity).

For claims 11 and 20, a computer storage medium having stored thereon a computer program readable by a general-purpose computer, which is equivalent to a

Art Unit: 2112

computer-readable medium storing a computer program arranged to condition a program-controlled computer (claim 14 of Mao).

For claims 13 and 15, a first computing entity is equivalent to a first computing entity in claim 11 of Mao, a second computing entity is equivalent to a second computing entity in claim 12 of Mao, and a communications network for communication the first and second entities is equivalent to "said communications equipment configured so as to communication data according to said set of instructions" (claims 11 and 12 of Mao)

For claims 23 and 26, claim 14 of Mao differs from these claims by a word "implementing". Implementing is equivalent to computing.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 10, 11, 13, 15, 19, 20, 23, and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Mao (GB 2372414 A).

Art Unit: 2112

For claim 10, the Examiner gives a broad interpretation of apparatus for carrying out the method of claim 1. Claim 11 of Mao includes all items for this apparatus (the first computing entity).

For claim 19, the Examiner gives a broad interpretation of apparatus for carrying out the method of claim 16. Claim 12 of Mao includes all items for this apparatus (the second computing entity).

For claims 11 and 20, a computer storage medium having stored thereon a computer program readable by a general-purpose computer, which is equivalent to a computer-readable medium storing a computer program arranged to condition a program-controlled computer (claim 14 of Mao).

For claims 13 and 15, a first computing entity is equivalent to a first computing entity in claim 11 of Mao, a second computing entity is equivalent to a second computing entity in claim 12 of Mao, and a communications network for communication the first and second entities is equivalent to "said communications equipment configured so as to communication data according to said set of instructions" (claims 11 and 12 of Mao)

For claims 23 and 26, claim 14 of Mao differs from these claims by a word "implementing". Implementing is equivalent to computing.

***Allowable Subject Matter***



Art Unit: 2112

Claims 21 and 24 are allowed. The following is a statement of reasons for the indication of allowable subject matter: The prior art does not disclose for specific steps of 21c and 24c ( steps a) to c) being repeated as necessary to obtain  $s||w \leq N_A$ ).

Claim 22 and 25 are allowed. They are dependent claim of claim 21 and 24.

### ***Conclusion***

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure. The prior arts disclose information about signcryption and probabilistic signature scheme.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2112

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le  
10/02/2006

  
WALTER D. GRIFFIN  
SUPERVISORY PATENT EXAMINER